

REPLACEMENT SHEET

20

CLAIMS

1. A method in a telecommunication system for allowing a
SIM-based authentication to users of a wireless local
area network who are subscribers of a public land
mobile network, the method comprising the steps of:
- 5
- (a) a wireless terminal accessing the wireless local
area network through an accessible Access Point;
- (b) discovering an Access Controller interposed between
the Access Point and the public land mobile network
from the wireless terminal;
- 10
- (c) carrying out a challenge-response authentication
procedure between the wireless terminal and the
public land mobile network through the Access
Controller, the wireless terminal provided with a
SIM card and adapted for reading data thereof;
- 15
- the method **characterized in that** the challenge-response
authentication submissions in step c) take place
before having provided IP connectivity to the user, and
are carried:
- 20
- on top of a Point-to-Point layer 2 protocol
(PPPoE) between the wireless terminal and the
Access Controller; and
 - on an authentication protocol residing at
application layer between the public land
mobile network and the Access Controller; and
- 25
- the method further comprises a step of:
- (d) offering IP connectivity to the user at the
wireless terminal, by sending an assigned IP
address and other network configuration parameters,

REPLACEMENT SHEET

21

once said user has been validly authenticated by the public land mobile network.

2. The method in claim 1, wherein the step b) of discovering an Access Controller includes a step of establishing a Point-to-Point Protocol session between a Point-to-Point over Ethernet (PPPoE) Protocol client in the wireless terminal and a Point-to-Point over Ethernet (PPPoE) Protocol server in the Access Controller.
3. The method in claim 1, wherein the step c) of carrying out the challenge-response authentication procedure include the steps of:
- (c1) sending a user identifier from the wireless terminal to the public land mobile network through the Access Controller;
 - (c2) receiving an authentication challenge at the wireless terminal from the public land mobile network via the Access Controller;
 - (c3) deriving encryption key and authentication response at the wireless terminal from the received challenge;
 - (c4) sending the authentication response from the wireless terminal to the public land mobile network through the Access Controller;
 - (c5) receiving at the Access Controller an encryption key from the public land mobile network; and
 - (c6) extracting the encryption key received for further encryption of communication path with the wireless terminal.

REPLACEMENT SHEET

22

4. The method in claim 2, further comprising a step of shifting authentication information received on top of a Point-to-Point layer 2 protocol (PPPoE) upwards to an authentication protocol residing at application layer for submissions toward the public land mobile network.
5
5. The method in claim 4, further comprising a step of shifting authentication information received on an authentication protocol residing at application layer downwards on top of a Point-to-Point layer 2 protocol (PPPoE) for submissions toward the wireless terminal.
10
6. The method in claim 3, further comprising a step of establishing at the wireless terminal a symmetric encryption path by using the previously derived encryption keys at the Access Controller and wireless terminal.
15
7. The method in any preceding claim, wherein the step d) of sending an IP address includes a previous step of requesting such IP address from a Dynamic Host Configuration Protocol server.
- 20 8. The method in any preceding claim, wherein the communication between the Access Controller and the public land mobile network goes through an Authentication Gateway of said public land mobile network.
- 25 9. The method in any preceding claim, wherein the communication between the Access Controller and the Authentication Gateway of a public land mobile network goes through an Authentication Server of the wireless local area network in charge of authenticating local users of said wireless local area network who are not
30 mobile subscribers.

REPLACEMENT SHEET

23

10. The method in any preceding claim, wherein the user identifier in step c1) comprises a Network Access Identifier.
- 5 11. The method in any preceding claim, wherein the user identifier in step c1) comprises an International Mobile Subscriber Identity.
12. The method in any preceding claim, wherein the authentication protocol residing at application layer in step c) is an Extensible Authentication Protocol.
- 10 13. The method in claim 12, wherein this Extensible Authentication Protocol is transported over a RADIUS protocol.
14. The method in claim 12, wherein this Extensible Authentication Protocol is transported over a Diameter protocol.
- 15 15. An Access Controller in a telecommunication system that comprises a wireless local area network including at least one Access Point, a public land mobile network, and at least one Terminal Equipment provided with a SIM card and adapted for reading subscriber data thereof, the Access Controller characterized in that it comprises:
- 20 (a) a Point-to-Point layer 2 protocol (PPPoE) server for communicating with the wireless terminal, and arranged for tunneling the challenge-response authentication procedure; and
- 25 (b) an authentication protocol residing at an OSI application layer for communicating with the public land mobile network.
- 30 16. The Access Controller in claim 15 further comprising:

AMENDED SHEET

REPLACEMENT SHEET

24

- (a) means for shifting the information received on top of the Point-to-Point layer 2 protocol (PPPoE) upwards to the authentication protocol residing at application layer; and
- 5 (b) means for shifting the information received on the authentication protocol residing at application layer downwards on top of the Point-to-Point layer 2 protocol (PPPoE).
- 10 17. The Access Controller in claim 16 further comprising means for requesting an IP address from a Dynamic Host Configuration Protocol server, after a user has been successfully authenticated by his public land mobile network.
- 15 18. An Access Controller according to claim 17 adapted for communicating with a wireless terminal via an Access Point.
19. An Access Controller according to claim 17 adapted for communicating with a public land mobile network via an Authentication Gateway.
- 20 20. An Access Controller according to claim 17 adapted for communicating with an Authentication Gateway via an Authentication Server responsible for authenticating local users of a wireless local area network.
- 25 21. An Access Controller according to any of claims 15 to 20, wherein the authentication protocol residing at application layer is an Extensible Authentication Protocol.
- 30 22. The Access Controller in claim 21, wherein this Extensible Authentication Protocol is transported over a RADIUS protocol.

REPLACEMENT SHEET

25

23. The Access Controller in claim 21, wherein this Extensible Authentication Protocol is transported over a Diameter protocol.
- 5 24. A wireless terminal comprising functionality for acting as a Point-to-Point layer 2 protocol (PPPoE) client and having an Extensible Authentication Protocol on top of this Point-to-Point layer 2 protocol.
- 10 25. A telecommunication system comprising a wireless local area network that includes at least one Access Point, a public land mobile network, and at least one Terminal Equipment provided with a SIM card and adapted for reading subscriber data thereof, **characterized in that** it further comprises the Access Controller in claims 15 to 23 for allowing SIM-based subscriber authentication to users of the wireless local area network who are subscribers of the public land mobile network.
- 15